WHAT IS CLAIMED IS:

1. An encryption apparatus, comprising:

an encryption processing unit configured to iterate a specified operation in order to encrypt data and to externally output the encrypted data, said encryption processing unit, including:

a non-linear transformation circuit configured to non-linearly transform an input first data block based on input key information and configured to output the non-linearly transformed result value,

a logical operation circuit configured to logically operate on the non-linearly transformed result value and an input second data block and configured to output the logical operated result value, and

a substitution module configured to substitute said second data block with said first data block and said first data block with the logical operated result value; and

a changing module configured to change said key information input into said non-linear transformation circuit into a value unrelated to said key information,

wherein said changing module begins execution after said encrypted data is output from said encryption processing unit.

2. An encryption apparatus comprising:

an encryption processing unit configured to iterate a specified operation in order to encrypt data and to externally output the encrypted data, said encryption processing unit, including:

a non-linear transformation circuit configured to non-linearly transform an input first data block based on input key information and configured to

18

output the non-linearly transformed result value,

a logical operation circuit configured to logically operate the non-linearly transformed result value and an input second data block and configured to output the logical operated result value, and

a substitution module configured to substitute said second data block with said first data block and said first data block with the logical operated result value; and

a first changing unit configured to change said first data block input into said non-linear transformation circuit into a value unrelated to said first data block,

wherein said first changing unit begins execution after said encrypted data is output from said encryption processing unit.

3.   An apparatus according to claim 2, further comprising

a second changing unit configured to change said key information input into said non-linear transformation circuit into a value unrelated to said key information, wherein said second changing unit starts execution after said encrypted data is output from said encryption processing unit.

4.   An encryption apparatus comprising:

an encryption operation unit configured to perform a non-linear function, said encryption operation unit being provided with a Feistel type encryption algorithm and configured to output encrypted data; and

a changing unit configured to change a result of an encryption operation into irrelevant data for output to the non-linear function,

wherein said changing unit starts changing the result into said irrelevant data

19

after said encrypted data is output.

5. An encryption apparatus according to claim 4, wherein said irrelevant data is data used to change key information which is to be provided to the non-linear function.

6. An encryption apparatus according to claim 4, wherein said irrelevant data is data used to change a first block data which is to be applied to the non-linear function.

7. An encryption apparatus provided with a Feistel type encryption algorithm including a non-linear transformation, comprising:

a register storing data in the encryption apparatus; and

a changing unit configured to change a data block to be applied to said non-linear transformation into a value unrelated to the data block in order to supply the register with information unrelated to an encryption process,

wherein said changing unit begins execution after said encrypted data is output.

8. An encryption apparatus provided with a Feistel type encryption algorithm including a non-linear transformation, comprising:

a register storing data in the encryption apparatus; and

a changing unit configured to change key information to be applied to said non-linear transformation into a value unrelated to the key information in order to supply the register with information unrelated to an encryption processing,

wherein said changing unit begins execution after said encrypted data is output.

9.   An encryption apparatus according to claim 8, further comprising

a second changing unit configured to change a data block to be applied to said non-linear transformation into a value unrelated to the data block in order to supply said register with information unrelated to said encryption processing, wherein said second changing unit starts execution after said encrypted data is output.

10.   A method for encrypting data in an encryption apparatus utilizing a Feistel type encryption algorithm, comprising:

receiving data to be encrypted;

performing an encryption operation on the received data to produce encrypted data;

outputting the encrypted data;

changing the encrypted data into irrelevant data immediately after outputting the encrypted data; and

performing a non-linear operation on the irrelevant data.